Math 106: Problem Set 4

Owen Jones

2/18/2024

Prime Divisor Property

Let p be prime, and suppose $p \mid ab$.
WLOG assume $p \nmid a$. We want to show $p \mid b$. Since the only factors of p are 1 and p, if $p \nmid a$, then $\gcd(p, a) = 1$. It follows there exists integers m, n s.t $am + pn = 1$. It follows $abm + bpn = b$. Since $p \mid bpn$ and $p \mid abm$, p must divide a linear combination of bpn and abm. Hence, $p \mid b$.

Fundamental Theorem of Arithmetic

Part 1: prime factorization of n
Pf by induction
Base case: $n = 2$ is a prime number, so its factors are 1 and itself. Thus, it's prime factorization is 2.
Induction hypothesis: Assume for some $n > 2$ that every integer k s.t $2 \leq k < n$ can be factored into a product of primes.
Induction step: We want to show n can be factored into a product of primes.
The case where n is a prime is trivial. Its factorization is just n. Suppose n is not a prime. THus, n has a proper divisor. Let $d \mid n$ where $d \neq n$. It follows there exists an integer k s.t $dk = n$. Since both d and k are less than n, the induction hypothesis states that d and k can be written as a product of primes. Thus, n can be written as a product of primes. Hence, by induction, every integer 2 or greater can be written as a product of primes.

Part 2: Uniqueness of the prime factorization
Pf by contradiction
Assume to the contrary the prime factorization of n is not unique.
Let $n = p_1p_2 \dots p_k$ and $n = q_1q_2 \dots q_m$ be prime factorizations for n. Let $s_1, s_2, \dots, s_l$ be the shared prime factors between the two factorizations.
We relabel and reindex each factorization as $n = s_1s_2 \dots s_l p^*_{l+1} \dots p^*_k$ and $n = s_1s_2 \dots s_l q^*_{l+1} \dots q^*_m$. By assuption, there exists some $p^*_i \notin \{q^*_{l+1}, \dots, q^*_m\}$. However, $p_{\mid \frac{n}{s_1s_2 \dots s_l}} = q^*_{l+1} \dots q^*_m$, so $p_i = q_j$ for some $j = l+1, \dots m$. Thus, we obtain a contradiction because $p^*_i \notin \{q^*_{l+1}, \dots, q^*_m\}$. Hence, n has a unique prime factorization.

5.2.1 Suppose $mp \equiv 1 \pmod{a}$. It follows there exists some integer k s.t $mp - ak = 1$. Because $mp - ak$ is a linear combination of p and a, $\gcd(p, a) \mid mp - ak$. Thus, $\gcd(p, a) \mid 1$. However, the only divisor of 1 is itself, so

$\gcd(p, a) = 1$.

5.2.2 Suppose $m_1, \dots m_k$ be pairwise relatively prime integers and let x be an integer that satisfies the following system of congruence relations:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\dots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

Let $M = \prod m_i$ and let $z_i = \frac{M}{m_i}$. Because z_i and m_i are relatively prime, Bezout's identity says there exists an integer y_i s.t $y_i z_i \equiv 1 \pmod{m_i}$. It follows $a_i y_i z_i \equiv a_i \pmod{m_i}$. For any i, j s.t $i \neq j$ $m_j \mid z_i$, so $a_i y_i z_i \equiv 0 \pmod{m_j}$. Thus, $x = \displaystyle\sum_{i=1}^{k} a_i y_i z_i$ is a solution to the system of congruence relations.
Let x_1, x_2 both be solutions to the system of congruence relations. It follows

$$\begin{aligned} x_1 &\equiv x_2 \pmod{m_1} \\ x_1 &\equiv x_2 \pmod{m_2} \\ &\dots \\ x_1 &\equiv x_2 \pmod{m_k} \end{aligned}$$

Because $m_i \mid x_1 - x_2$ for all $i = 1 \dots k$ and the m_i's are relatively prime, $M \mid x_1 - x_2$. Thus, the solution $x = \displaystyle\sum_{i=1}^{k} a_i y_i z_i$ is unique $\pmod{M}$.

5.3.1

	x	y
21	1	0
17	0	1
4	1	-1
1	-4	5

$\Rightarrow 17 \cdot 5 - 21 \cdot 4 = 1$

5.3.2 $17 \cdot 15 - 21 \cdot 12 = 3$

5.4.2 Suppose (x_1, y_1, k_1) and (x_2, y_2, k_2) are solutions to $x^2 - Ny^2 = k$.
We are given $k_1 k_2 = (x_1^2 - Ny_1^2)(x_2^2 - Ny_2^2)$
$= (x_1 - \sqrt{N} y_1)(x_1 + \sqrt{N} y_1)(x_2 - \sqrt{N} y_2)(x_2 + \sqrt{N} y_2)$.

$$
\begin{aligned}
(x_1 - \sqrt{N}y_1)(x_2 - \sqrt{N}y_2) &= x_1x_2 - \sqrt{N}(x_1y_2 + x_2y_1) + Ny_1y_2 \\
&= (x_1x_2 + Ny_1y_2) - \sqrt{N}(x_1y_2 + x_2y_1) \\
(x_1 + \sqrt{N}y_1)(x_2 + \sqrt{N}y_2) &= x_1x_2 + \sqrt{N}(x_1y_2 + x_2y_1) + Ny_1y_2 \\
&= (x_1x_2 + Ny_1y_2) - \sqrt{N}(x_1y_2 + x_2y_1) \\
\Rightarrow k_1k_2 = (x_1^2 - Ny_1^2)(x_2^2 - Ny_2^2) &= (x_1x_2 + Ny_1y_2)^2 - N(x_1y_2 + x_2y_1)^2
\end{aligned}
$$

5.4.3 A positive integer is a perfect square if and only if every prime in its factorization occurs an even number of times. Let N be a nonsquare integer. By the Fundamental Theorem of Arithmetic, N can be written as a product of primes. It follows there exists some prime p that occurs an odd number of times. Assume to the contrary that $\sqrt{N} = \frac{a}{b}$ is rational, where $a, b \in \mathbb{Z}$ are relatively prime and $b > 0$. Squaring both sides and multiplying by b^2, we obtain $b^2N = a^2$. Because b^2 is a perfect square, p occurs an even number of times in its prime factorization. Thus, p occurs an odd number of times in the prime factorization of b^2N. However, p must occur an even number of times in the prime factorization of a^2 because a^2 is also a perfect square, so by the uniqueness of a number's prime factorization, we obtain a contradiction. Hence, $\sqrt{N}$ cannot be rational.
Assume to the contrary $a_1 - \sqrt{N}b_1 = a_2 - \sqrt{N}b_2$, but $a_1 \neq a_2$ or $b_1 \neq b_2$. Suppose WLOG $b_1 \neq b_2$. It follows $\sqrt{N} = \frac{a_1 - a_2}{b_1 - b_2}$. However, N is not a perfect square, so $\sqrt{N}$ is irrational. Because $a_1, a_2, b_1, b_2 \in \mathbf{Z} \Rightarrow \frac{a_1 - a_2}{b_1 - b_2} \in \mathbb{Q}$ which is a contradiction, so $b_1 = b_2$. Suppose $a_1 \neq a_2$. Since $b_1 = b_2 \Rightarrow \sqrt{N}b_1 = \sqrt{N}b_2$. It follows $a_1 - \sqrt{N}b_1 \neq a_2 - \sqrt{N}b_2$ which is a contradiction, so $a_1 = a_2$.

5.4.4 $(x_1 - \sqrt{N}y_1)(x_2\sqrt{N}y_2) = (x_1x_2 + Ny_1y_2) - \sqrt{N}(x_1y_2 + x_2y_1)$. By **5.4.3** $(x_1x_2 + Ny_1y_2) - \sqrt{N}(x_1y_2 + x_2y_1) = x_3 - \sqrt{N}y_3 \Rightarrow x_1x_2 + Ny_1y_2 = x_3$ and $x_1y_2 + x_2y_1 = y_3$.

6.3.1 Let L be the line through rational points $p_1 = (x_1, y_1)$ and $p_2 = (x_2, y_2)$. We can define L by the equation $(y - y_1)(x_2 - x_1) = (y_2 - y_1)(x - x_1)$. Because $x_1, x_2, y_1, y_2 \in \mathbb{Q}$, the addition, subtraction, multiplication, and nonzero division of x_1, x_2, y_1, y_2 are rational. Moreover, the coefficients of $(x_2 - x_1)y + (y_1 - y_2)x = y_1x_2 - y_2x_1$ are all rational.

6.3.2 Let the center of the circle be $c = (x_1, y_1)$ with point on the radius $r = (x_2, y_2)$. Define the equation for the circle, $(x - x_1)^2 + (y - y_1)^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2$. Because $x_1, x_2, y_1, y_2 \in \mathbb{Q}$, the addition, subtraction, multiplication, and nonzero division of x_1, x_2, y_1, y_2 are rational. Thus, $x^2 - 2x_1x + x_1^2 + y^2 - 2y_1y + y_1^2 = x_2^2 - 2x_1x_2 + x_1^2 + y_2^2 - 2y_1y_2 + y_1^2$ are all rational.

6.3.3 Define the lines $\ell_1 : a_1x + b_1y = c_1, \ell_2 : a_2x + b_2y = c_2$. Suppose they intersect at some point (x^*, y^*).
By elimination, we obtain $(a_2b_1 - a_1b_2)y = a_2c_1 - a_1c_2 \Rightarrow y^* = \frac{a_2c_1 - a_1c_2}{a_2b_1 - a_1b_2}$.
$\ell_1 \parallel \ell_2$ if $a_1b_2 = a_2b_1$. Plugging in y^* into one of the two equations, we can solve for $x^* = \frac{b_2c_1 - b_1c_2}{a_1b_2 - a_2b_1}$.

6.3.4 The case of the vertical line $x = c$ is a simpler case where the line and circle intersect at $(c, k + \sqrt{r^2 - (c-h)^2}), (c, k - \sqrt{r^2 - (c-h)^2})$.
Suppose a line $y = mx + b$ and circle $(x-h)^2 + (y-k)^2 = r^2$ intersect at some point(s).
Substituting y with $mx + b$ we get $(x-h)^2 + (mx + b - k)^2 = r^2$.

$$
\begin{aligned}
&\text{let } c = b - k \\
x^2 - 2hx + h^2 + m^2x^2 + 2cmx + c^2 - r^2 &= 0 \\
(m^2+1)x^2 + (2cm - 2h)x + h^2 + c^2 - r^2 &= 0 \\
x^* = \frac{h - cm \pm \sqrt{-2cmh - m^2h^2 - c^2 + m^2r^2 + r^2}}{m^2+1}& \\
x^* = \frac{h - (b-k)m \pm \sqrt{r^2(m^2+1) - (b - k + mh)^2}}{m^2+1}&
\end{aligned}
$$

so we can find solutions for x^* using only rational equations and square roots. Plugging the solutions for x^* into $y = mx + b$ we can find the corresponding y^* values.

6.4.1 Assume to the contrary $\sqrt[3]{2} = \frac{a}{b}$ is rational where a and b are coprime. Cubing both sides and multiplying by b^3 we obtain $2b^3 = a^3$. It follows $2 \mid a^3$ and by the FTA $2 \mid a$. Thus, there exists some integer a' s.t $a = 2a'$. This implies $b^3 = 4a'^3 \Rightarrow 2 \mid b^3$, and once again, by the FTA $2 \mid b$. However, $2 \mid a$ and $2 \mid b$, so we obtain a contradiction because we originally stated a and b are coprime.

6.4.2 Proof by induction
Base case: The set of rational numbers is trivially a field.
Induction hypothesis: Assume for some k that F_k is a field.
Induction step: Let $x = a_1 + b_1\sqrt{c_{k1}}, y = a_2 + b_2\sqrt{c_k}$
$x + y \in F_{k+1}$ because $a_1 + a_2, b_1 + b_2, c_k \in F_k$
$x - y \in F_{k+1}$ because $a_1 - a_2, b_1 - b_2, c_k \in F_k$
$xy \in F_{k+1}$ because $a_1a_2 + b_1b_2c_k, a_1b_2 + a_2b_1, c_k \in F_k$
$\frac{x}{y} \in F_{k+1}$ because $\frac{a_1a_2 - b_1b_2c_k}{a_2^2 - b_2^2c_k}, \frac{a_2b_1 - a_1b_2}{a_2^2 - b_2^2c_k}, c_k \in F_k$
Hence, by induction, the claim holds for all k.